ESG SHOWCASE

NG-IDS, NDR, and ExtraHop

Date: April 2021 **Author:** Jon Oltsik, Senior Principal Analyst and Fellow

ABSTRACT: Large enterprises have employed IDS systems since the 1990s, typically at the network perimeter to inspect traffic for exploits targeting software vulnerabilities/CVEs. Meanwhile, a lot has changed over the past 20+ years, including the nature of cyber-threats, de-perimeterization, expanding encryption blindspots, and a growing attack surface. When CISOs examine the role and function of IDS, they will discover that they really need something more—a next-generation intrusion detection system (NG-IDS) solution with more comprehensive visibility, better threat detection efficacy, and tighter integration with security operations.

Overview

According to ESG research, 85% of organizations believe network security is more difficult today than it was 2 years ago due to factors like:[1]

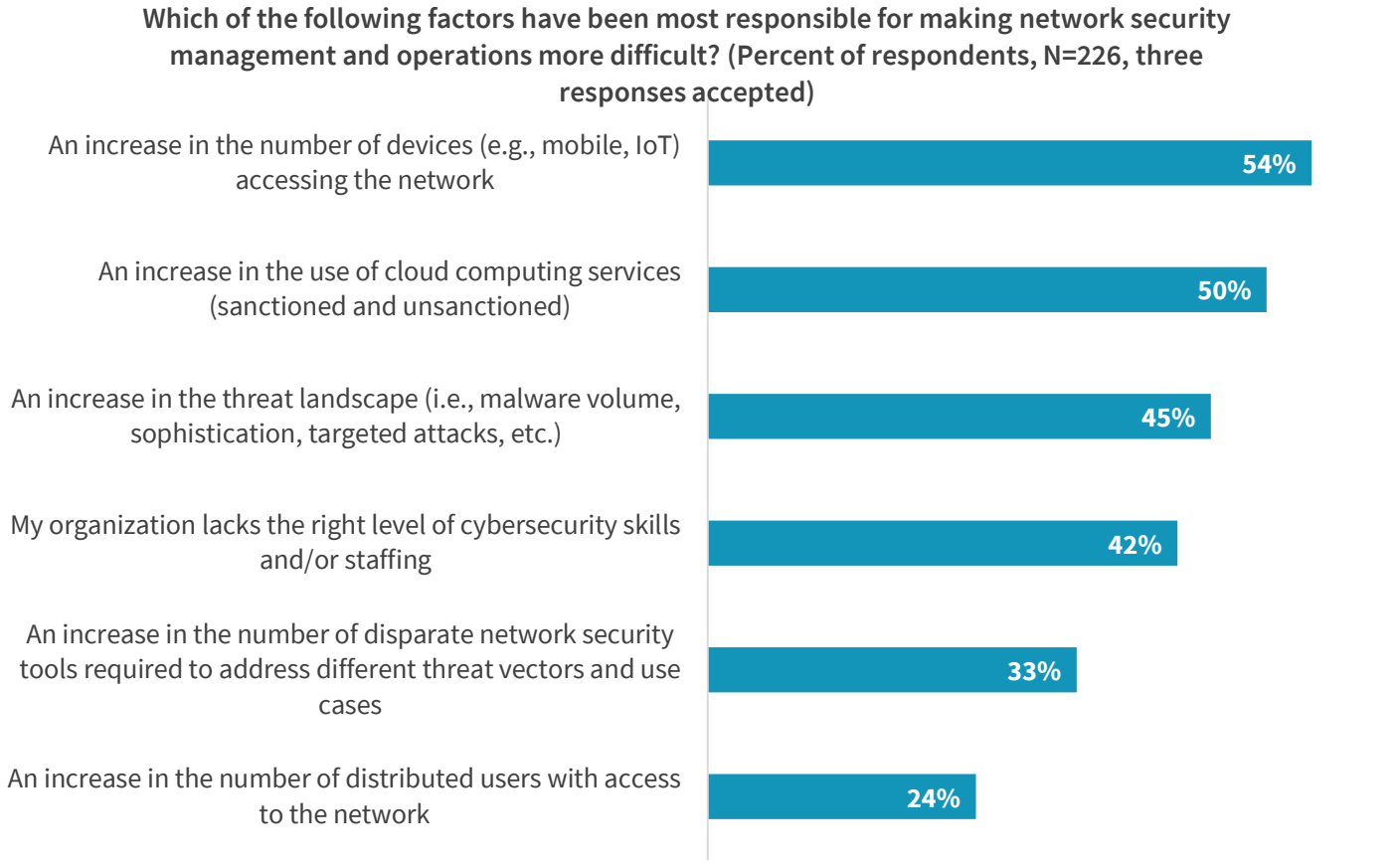
- Network complexity. Corporate networks now extend to multiple public cloud providers, carrier networks, and even consumer Wi-Fi devices used by remote workers. Somehow, the security and IT team must secure and monitor all traffic, including encrypted, to prevent, detect, and respond to network-based cyber-attacks.
- The dangerous threat landscape. Organizations face unprecedented cyber-threats, from phishing, to ransomware, to cyber-supply chain interdiction. In fact, attackers have modified their strategies, using social engineering techniques against human targets rather than rely on exploiting software vulnerabilities as they did in the past. Network security plays an essential role in detecting these threats, but this has become more difficult due to their volume and sophistication.
- A growing attack surface. Over the past 2 years, most organizations have moved workloads to the cloud, embraced SaaS applications, deployed IoT devices, and increased the population of remote employees. Overwhelmed security teams must further extend resources to protect this growing attack surface.

It is also worth noting that 42% of respondents say that network security is more difficult due to the global cybersecurity skills shortage (see Figure 1). This is understandable as network complexity and the expanding attack surface create more work for network security teams, but these teams are often understaffed and lacking in advanced skills. Additionally, one-third of respondents (33%) claim that network security has become more difficult because of an increase in the number of disparate network security tools necessary to prevent, detect, and respond to cyber-threats.[2] Combining these two data points, there is a shortage of cybersecurity personnel and an abundance of network security tools—a poor combination for scaling network security operations.

[1] Source: ESG Research Report, *The State of Network Security: A Market Poised for Transition*, March 2020.

[2] Ibid.

Figure 1. Reasons Why Network Security Has Become More Difficult Over the Last 2 Years



Source: Enterprise Strategy Group

As network security grows more difficult, CISOs realize that they can't rely on legacy strategies and technologies. Therefore, organizations are seeking new network security solutions for threat prevention, detection, and response featuring:

- High efficacy: Security operations teams don't have the time or resources to sort through logs or triage voluminous security alerts from noisy network security tools. Rather, network security technology must be able to accurately detect threats in real time across the enterprise and throughout the attack kill chain.
- Operational efficiency. Overburdened security teams can't scale operations when network security is based on individual network security tools requiring training, complex deployment, system tuning, and ongoing administration. Henceforth, independent network security systems must be designed to support security operations processes like forensic investigations, threat hunting, incident response, process automation, etc. This is an important change that emphasizes global security operations rather than each security technology.
- Tight integration. Given the growing attack surface and distributed network, it's not surprising that security teams strive for interoperability amongst all network security technologies. In fact, 84% of organizations say that they are very active or somewhat active with efforts to integrate disparate security analytics and operations tools to form a more cohesive security software architecture.[3]

[3] Source: ESG Research Report, *The Rise of Cloud-based Security Analytics and Operations Technologies*, December 2019.

- Minimize dwell time. Network security technology must provide detection-in-depth to identify different types of attacks (i.e., phishing, cyber-supply chain attacks, stolen credentials, etc.) regardless of their location or phase of the kill chain. The goal? Greatly reduce mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) cyber-attacks before any real damage is done. To accomplish this, network security technologies must also help security teams operationalize the MITRE ATT&CK framework.

What About IDS?

As CISOs push a new direction for network security, they must examine each network security piece to determine whether to include it in their integration plans or seek alternative solutions. This question is especially relevant regarding IDS, a technology with its roots in the 1990s designed to protect against things like port scanning, SQL injections, and buffer overflows that exploited software vulnerabilities. As organizations pivot to a more modern and integrated network security model, traditional IDS becomes a mismatch because it:

- Is designed with a narrow view of threat detection efficacy. IDS threat detection capabilities are anchored by signatures, which assume an exact match when triggering an alert, while heuristics are designed to pick up slight deviations associated with known attacks. These detection methods can be a helpful defense against script kiddies but not sophisticated adversaries. Many organizations also report that at least 50% of network traffic is typically encrypted today, and this percentage will only increase in the future. Unfortunately, network encryption blinds IDS from inspecting traffic and judging whether it is suspicious, malicious, or benign. IDS is often evaluated based on the number of signatures and CVE vulnerability coverage. Unfortunately, these metrics have never been an accurate view of threat detection efficacy. Today, attackers prefer to exploit workers' weaknesses to establish beachheads and then proceed through multi-phased cyber-attacks over CVE exploits.

- Doesn't usually cover east/west traffic. IDS had a well-established position in the past, sitting behind firewalls and comparing ingress/egress network traffic to signatures and heuristics to look for cyber-attacks and policy violations. This activity is still worthwhile, but most organizations now rely on IDS services built into next-generation firewalls (NGFWs). This provides traditional IDS protection at the perimeter but doesn't help detect attacks exploiting other vectors like malware embedded in phishing email attachments, malicious links on trusted websites, or compromised systems of third-party partners. In these cases, threat detection depends upon east/west traffic inspection, but this means that organizations have to find more money for resources to install, configure, and operate a multitude of IDS appliances to gain this coverage. However, moving IDS further into the core network requires a rethinking of the signature strategy to apply. Today's attackers increasingly live off the land, using the landed host's tools indistinguishable to IDS. Also, assumptions of good and bad traffic from the internet do not always hold in the cloud and virtualized environments. For example, it is common for VMware ESXi elements to stuff ICMP payload as a means for inter VM communications, creating a storm of false positives from IDS.

- Doesn't help with network security hygiene. IDS is really designed for the single purpose of comparing network traffic to signature and simple heuristics, but network security requirements extend beyond this narrow use case. Organizations need to look for things like misconfigured systems, exposed administrator credentials, expired certificates, risky behavior, and compliance violations. Since IDS doesn't provide this coverage, security teams are forced to purchase, install, and operate additional tools.

- Creates operational overhead. IDS typically acts as a standalone technology that can be difficult to configure, tune, and operate. It is also known to be quite finicky. When SOC teams get too granular tuning signature sets, IDS can mistakenly bypass malicious traffic, but when signatures sets are too broad, IDS becomes especially noisy with false

positive alerts. Beyond signature/heuristic-based threat detection, IDS provides little support for other network operations tasks like forensic investigations, threat hunting, or incident response.

NG-IDS: Broader, Deeper, and Part of an Integrated Network Security Stack

IDS is still useful, but organizations need more than simple signature/heuristic matching on a subset of their network traffic. So, what's needed? Next-generation IDS (NG-IDS) built for modern network security requirements. NG-IDS addresses these needs by providing:

- End-to-end coverage. Beyond the perimeter, NG-IDS should be present to inspect traffic across the network (in data centers, public clouds, on the internal network, etc.), so it can continually monitor north/south AND east/west traffic. In addition, NG-IDS also accommodates encrypted traffic inspection, pinpoints, and reports on network hygiene issues, captures packets for detailed investigations, and works with malware sandboxes to collect and inspect file payloads for malicious payloads.

- Improved threat detection accuracy. Threat detection must extend past signatures and basic heuristics, using modern technologies like machine learning algorithms, predictive models, continuous content updates based on threat research, and cloud-scale analytics. The goal here is to bolster threat detection efficacy and accuracy, allowing analysts to prioritize investigation and remediation actions. To support forensic investigations, NG-IDS retains network security metadata for at least 90 days while providing the right dashboards and interfaces for junior and experienced security analysts from a single interface.

- Contextual alerting. Aside from accurate detection of individual security events, SOC teams want to associate individual events to detect and understand cyber-attacks as they progress across a cyber-kill chain. This requires an ability to correlate and contextualize security events and then view them with an understanding of network traffic behavior, threat intelligence, and attack patterns. The focus here is on damage prevention rather than security alerts alone. Therefore, NG-IDS must be designed to piece together attacker TTPs, not just discrete rules violations. To maximize value, NG-IDS also supports the MITRE ATT&CK Framework.

- Security operations affinity. NG-IDS is designed for out-of-the-box integration with security technologies and operational processes. For example, NG-IDS ingests data from different sources like cloud infrastructure and threat intelligence to be able to have perspective on network security events. NG-IDS also integrates with other analytics solutions like SIEM systems, feeding them high-fidelity alerts for further investigation. To streamline security operations, NG-IDS interoperates with IT infrastructure solutions, SOAR platforms, and IT operations case management systems. In aggregate, NG-IDS supplements, enhances, and accelerates existing technologies and processes.

NG-IDS should be tightly integrated into a broader network security stack that includes technologies for threat prevention, detection, and response. This alone can help organizations through their budgeting and procurement processes. Rather than continue to fund standalone IDS, CISOs can use those budget dollars to support the organization's primary security goals, namely cyber-risk reduction and critical asset protection.

ExtraHop NDR Can Help Modernize Network Security

ExtraHop provides NG-IDS functionality as part of its Reveal(x) network detection and response (NDR) platform. In this way, ExtraHop supports machine-learning behavioral analysis missing from traditional IDS then extends security with

technologies designed for east/west traffic visibility, insider threat analysis, security hygiene violation detection, and rules-based critical CVE exploit detection.

ExtraHop can help customers:

- Eliminate blind spots across the enterprise. Reveal(x) is a cloud native NDR platform that can take advantage of cloud scale, storage, and analytics capabilities, providing east/west traffic visibility and encrypted traffic inspection. For full coverage, ExtraHop NDR also discovers and classifies every transaction, session, device, and asset at up to 100Gbps, decoding over 70 enterprise protocols.
- Modernize threat detection. ExtraHop goes beyond traditional IDS signature and heuristic threat detection with machine learning across 5,000 different network metadata features, leading to more than one million different predictive models per site. ExtraHop supports these models with continuous updates based on emerging threat intelligence and research.
- Contextualize alerts and accelerate investigations. Reveal(x) contextualizes detections from an entire transaction with threat intelligence, risk scores, and asset criticality. The goal here is to provide analysts with accurate, actionable, high-fidelity alerts rather than security alerts related to individual anomalies and events.
- Streamline security operations. Reveal(x) provides visualizations and dashboards to go from visibility to detection to investigation to forensic proof on its own. Reveal(x) can be combined with solutions like CrowdStrike, Splunk SIEM/SOAR, and Palo Alto Networks for security operations orchestration and automation of response and containment actions.
- Start fast with SaaS-based security. Reveal(x) 360 takes a SaaS-based approach to delivering NG-IDS capabilities for hybrid and multi-cloud deployments. Organizations can deploy Reveal(x) 360 sensor to on-premises and cloud environments and gain unified visibility from a single detection and response service platform.

Reveal(x) is a comprehensive network security solution. So much so, in fact, that companies working with ExtraHop can consolidate IDS budgets with NDR and network forensics requirements, streamline procurement, and improve overall network security efficacy and efficiency. This alone should persuade CISOs to take a look at ExtraHop, Reveal(x), and its integrated NG-IDS functionality.

The Bigger Truth

IDS systems have long been a network security staple, but their role in overall security protection is growing increasingly limited. Yes, IDS can still guard against CVE exploits, but most cyber-attacks today target people rather than application vulnerabilities. Furthermore, IDS is typically deployed to just inspect north/south traffic, leaving organizations blind to cyber-attacks pivoting laterally, east/west across the network. Finally, IDS can be operationally complex, difficult to tune and operate.

Security teams can no longer support operationally intensive one-off technologies like IDS. Rather, they need integrated solutions that can help them improve threat prevention, detection, and response while streamlining security operations. NG-IDS is designed to do exactly this as part of a broader NDR solution. CISOs looking for this type of network security solution should evaluate ExtraHop Reveal(x).

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188